EXHIBIT 17

This is an archived version of the Chrome privacy notice. View the current privacy notice.

Google Chrome Privacy Notice

Archive date: June 21, 2016

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and Safe Browsing. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the Google Privacy Policy.

Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll call it out.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read this overview of Chrome's privacy controls.

Table of contents:

Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you're using.

Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the network actions prediction feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you've visited before.
- A list of permissions you have granted to websites.
- A searchable index of non-secure pages you visit. Secure (HTTPS) pages, like bank websites, aren't included.
- Thumbnail-sized screenshots of pages you visit most often.
- Cookies or data from websites you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can delete your browsing history information.

- You can clear your cookies and site data by visiting the Cookies and Site Data dialog at chrome://settings/clearBrowserData.

- You can stop Chrome from accepting cookies from Google or other sites. Learn more.

- You can review stored passwords in Chrome settings. Learn more.

- You can view and manage your stored Autofill information. Learn more.

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by signing in to Chrome. Signing in enables Chrome's synchronization feature.

How Chrome handles your information

Information for website operators. Sites that you visit using Chrome will automatically receive standard log information, including your system's IP address and data from cookies or similar technologies. In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

Prerendering. To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. Learn more.

Location. To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however,

on mobile devices, once you've granted the app permission to access your location, Chrome automatically shares your location with your default search engine. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The wi-fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your wi-fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

Updates. Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

Search features. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. This allows your search engine to improve your searching and browsing experience by automatically suggesting terms or URLs you may be looking for. Learn more. If Google is your default search engine, Chrome contacts Google when you start searching or when you change networks, so you can get the best local web address for sending search queries. If you are signed in to a Google site or signed in to Chrome and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google account.

Suggestion service. Suggestions are based on related web searches, your browsing history, and popular websites. If your default search engine provides a suggestion service, the browser sends the text you type in the address bar to the search engine. Learn more about the address bar prediction service.

Navigation assistance. When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

Autofill and password management. Chrome sends Google limited, anonymous information about the

web forms that you encounter, including a hashed URL of the web page and details of the form's structure, so that we can improve our Autofill and password management services. Some web forms handled by Chrome will offer you the option of Autofilling with cards from Google Payments. If you use a card from Google Payments or choose to save your credit card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Payments to protect you from fraud.

Usage statistics and crash reports. You can send usage statistics and crash reports to Google to help us improve our products. For users on our early release versions and on Chromebooks, usage statistics and crash reports are enabled by default. Usage statistics contain information such as preferences, button clicks, and memory usage. Usage statistics do not include web page URLs or personal information unless you have reached what seems to be a phishing or malware web page. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We might share aggregated, non-personal information from crash reports with third parties. Learn more.

Content licensing. To allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome provides a unique identifier to content partners and websites that use Adobe Flash Access. The identifier is stored on your system. You can disable this in Chrome settings, or reset the unique identifier's value by reinstalling the operating system. If you access HD content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. To verify your device, your Chromebook will share data about its hardware attributes with the website, and will use Verified Access to certify that its cryptographic keys are protected by Chrome hardware. Chrome will prompt you to allow or deny this verification check. Learn more.

Other Google services. This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the Chrome Privacy Whitepaper.

Identifiers in Chrome

Chrome includes a number of identifiers necessary to power features. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique

identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome and manage updates.

- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates both a unique token that is sent to Google when you first run and use the browser and, if you received or reactivated your copy of the Chrome browser as part of a promotional campaign, a non-unique promotional tag. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. Learn more.

- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. Learn more.

Signed-in Chrome mode

When you sign in to the Chrome browser or a Chromebook with your Google Account, your personal browsing data is saved on Google's servers and synced with your account. This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

These settings are automatically loaded for you anytime you sign in to Chrome on other computers and devices. To customize the specific information that you synchronize, use the “Settings” menu. Learn

more. You can see the amount of Chrome data stored for your Google Account and manage it on the Chrome Sync Dashboard. On the Dashboard, you can also disable synchronization completely and delete all the associated data from Google's servers. Learn more.

How Chrome handles your signed-in information

When you sync Chrome with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App History. Learn more.

You can change this setting on your Account History page or manage your private data whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt all of your synced data with your own sync passphrase. Learn more.

Incognito mode and guest mode

You can limit the information Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

Cookies. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the incognito or guest window.

Browser configuration changes. When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or guest mode.

Permissions. Permissions you grant in incognito mode are not saved to your existing profile.

Profile information. In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

Managing Users in Chrome

Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. Learn more.

You can also create a supervised user in Chrome with your Google Account. If you do, Google will synchronize and store information about the supervised user, like history and other settings, with your Google Account. You can view this information at chrome.com/manage.

Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first signs in to Chrome or starts browsing without signing in (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive standard log information, including an IP address and cookies.

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. Learn more.

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.

- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. Learn more. If this kind of software is detected, Chrome might offer you the option to download the Chrome Cleanup Tool to remove it.

- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe

Browsing warning page. The reports contain various data, like the potentially dangerous file you encountered, the URL and contents of the website, and the URL of the page that directed you to that site.

- If usage statistics are enabled in Chrome and you visit a site that we think could be potentially harmful, certain additional data will be shared with Google, including the full URL that you visited, the "referrer" header sent to that page, and the URL that matched the Safe Browsing list.

- You can always choose to disable the Safe Browsing feature within Chrome.

Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the Google Privacy Policy unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

More information

Information that Google receives when you use Chrome is used and protected under the Google Privacy Policy. Information that other website operators and add-on developers receive, including cookies, is subject to the privacy policies of those websites.

Google adheres to several self-regulatory frameworks, including the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce. Learn more.

Definitions

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Other technologies are used for similar purposes as a cookie on other platforms where cookies are not available or applicable, such as the Advertising ID available on Android mobile devices. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

Google Account

You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or terminate your account at any time through your Google Account settings.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- `25/Mar/2003 10:15:32` is the date and time of the query;
- `https://www.google.com/search?q=cars` is the requested URL, including the search query;
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used; and
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to

the user the next time s/he visits Google from that particular computer).